



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/506,765

04/14/2005

Yongmao Li

11005.0064-00000

8915

97664 7590 08/16/2010
Huawei Technologies Co., Ltd./Finnegan
901 New York Avenue
NW
Washington, DC 20001

EXAMINER

OKEKE, IZUNNA

ART UNIT

PAPER NUMBER

2432

MAIL DATE

DELIVERY MODE

08/16/2010

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/506,765	Applicant(s) LI ET AL.	
	Examiner IZUNNA OKEKE	Art Unit 2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 01 June 2010.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3 and 6-26 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3 and 6-26 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Arguments

1. Applicant's arguments with respect to claims 1-3 and 6-26 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-3 and 10-26 are rejected under 35 U.S.C. 102(b) as being anticipated by Zhang et al. (US-20020174335).

a. *Referring to claim 1, 25 and 26:*

Regarding claims 1, 25 and 26, Zhang teaches a method for distributing encryption keys in a Wireless Local Area Network (WLAN), comprising: receiving, by an authentication device, an authentication request containing identification information for identity authentication from a mobile host (Para 76... authentication server receives authentication request comprising identification for user); authenticating said mobile host according to said identification information (Para 77-80... authentication according to the identification information); if authentication fails, sending a message comprising ACCESS_REJECT information to said mobile host, and if authentication succeeds: sending key-related information M1 to an access point (AP) wherein the key-related information M1 includes property information associated with the mobile host (Para 81-82... access_reject upon authentication failure and upon authentication success, sending a packet wherein the packet comprises user public key and

Art Unit: 2432

encrypted password identifier) [[,]] generating, by said AP, a key based on said key-related information M1 using a key generation algorithm; and sending a message comprising ACCESS ACCEPT information to said mobile host (Para 82... AP generating a key based on the information received from the server and sending access_accept packet to the mobile user), wherein: if the message comprising the ACCESS ACCEPT information comprises key-related information M2 including said key generated by said AP said key-related information M2 is encrypted by the AP and is sent to said mobile host along with said ACCESS ACCEPT information (sending access_accept packet to the mobile comprising the key, the user password encrypted with the PK); and if the message comprising the ACCESS ACCEPT information does not comprise the key-related information M2, the mobile host generates the key upon receipt of said message comprising the ACCESS ACCEPT information (Para 82... user computes the key by decrypting encrypted information in access_accept message).

a. Referring to claim 2:

Regarding claim 2, Zhang teaches the method of claim 1, wherein the mobile host generates the key according to property information stored in the mobile host with the same key generation algorithm after said mobile host receives said message comprising the ACCESS ACCEPT information (Para 82... user generates the key by decrypting the information using a private key of the public key used in encrypting the information).

a. Referring to claim 3:

Regarding claim 3, Zhang teaches the method of claim 1, wherein said mobile host obtains the key through decrypting the key-related information M2 (See the rejection in claim 2).

a. Referring to claims 10, 11, 12, 13 and 14:

Art Unit: 2432

Regarding claims 10, 11, 12, 13 and 14, Zhang teaches the method for distributing encryption keys in the WLAN of claim 1 wherein said authentication device is an authentication server installed in external network (Fig 1... authentication server in external network)..

a. Referring to claims 15, 16, 17, 18 and 19:

Regarding claims 15, 16, 17, 18 and 19, Zhang teaches the method for distributing encryption keys in the WLAN of claim 1 wherein said authentication device is a wireless gateway that connects said AP with external network (Para 47... authentication and billing gateway as the RADIUS server).

a. Referring to claims 20, 21, 22, 23 and 24:

Regarding claims 20, 21, 22, 23 and 24, Zhang teaches the method for distributing encryption keys in the WLAN of claim 1 wherein said authentication device includes a wireless gateway and said authentication server installed in external network (Fig 1. authentication server and gateway in the external network).

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Claims 6-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zhang et al. (US-20020174335), and further in view of Wang et al. (US-20030084287).

a. Referring to claim 6-9:

Regarding claim 6-9, Zhang teaches a method of distributing encryption keys wherein a mobile client authenticates to an authentication server using an identifier and upon successful authentication, the authentication server send key information to the AP to generate a key and the

Art Unit: 2432

mobile device can decrypt the key send from the AP. Zhang does not teach a key update method wherein the derived key is updated by generating a new key using a shared secret. However, periodically or aperiodically updating session keys or encryption keys used in communication between two entities is widely know in the art for ensuring the integrity of keys incase they have been compromised or fraudulently obtained by a hacker. For instance, Wang et al. discloses a method for authenticating a roaming device within a network and distributing encryption keys wherein the key is periodically updated to increase the security of the system. The AP (or the AS in another embodiment) generates the new key (update key) from the shared secret and send it to the client which derives the key from the shared secret. (See Wang, Para 26-28..... process for periodically updating the encryption key in a network). Therefore, one of ordinary skill in the art would be motivated to modify Zhang's system by adding a key update process as taught by Wang for the purpose of increasing the security of the system against a compromised key because if an encryption key is used repeatedly without updating or renewal, an attacker who successfully compromises the key will have access to the encrypted communications.

a. Referring to claim 6:

Regarding claim 6, the combination of Zhang and Wang teaches the method for distributing encryption keys in the WLAN of claim 1 wherein when receiving data packets encrypted with a key sent from the mobile host, said AP updates the key through the following steps of: (a1) said AP generating a random number and generating a new key from said random number with any key generation algorithm; (b1) said AP adding said random number to a key update message and then sending said message to said mobile host; (c1) when receiving said key update message, said mobile host generating a new key from said random number contained in

Art Unit: 2432

said key update message with the same key generation algorithm as that in step (a1); (d1) said mobile host encrypting the data packets to be sent to said AP with said new key and then sending the encrypted data packets to said AP, during the encryption process, said mobile host adding an encryption identifier to said data packets and changing the value of said encryption identifier to indicate the communication key has been changed; and (e1) when receiving the data packets from said mobile host, said AP determines whether to change the key according to value of said encryption identifier (See Wang, Para 26-28.... key update process carried out by AP wherein a new key is generated from a shared secret and sent to a mobile which obtains the new key from the shared secret wherein the new key is used for encrypting communication between the AP and client).

a. Referring to claim 7:

Regarding claim 7, the combination of Zhang and Wang teaches the method for distributing encryption keys in the WLAN of claim 1 wherein in order to achieve encryption communication with the new key, when receiving the data packets encrypted with the key sent from said mobile host, said AP updates the key periodically or aperiodically through the following steps of: (a2) said AP generating a new key in any way and encrypting said new key with the present key; (b2) said AP adding the encrypted key to the key update message and then sending said message to said mobile host; (c2) when receiving said key update message, said mobile host decrypting the new key contained in said key update message with the present key so as to obtain said new key; (d2) said mobile host encrypting the data packets to be sent to said AP with said new key and then sending the encrypted data packets to said AP, during the encryption process, said mobile host adding an encryption identifier to said data packets and

Art Unit: 2432

changing the value of said encryption identifier to indicate the communication key has been changed; and (e2) when receiving the data packets from said mobile host, said AP determines whether to change the key according to value of said encryption identifier (See the rejection in claim 6 and Wang, Para 26..... periodically updating the key)

a. Referring to claim 8:

Regarding claim 8, the combination of Zhang and Wang teaches the method for distributing encryption keys in the WLAN of claim 1 wherein when receiving the data packets encrypted with the key sent from said mobile host, said AP updates the key periodically or aperiodically through the following steps of: (a3) said authentication device generating a random number which is used to generate a new key with the key generation algorithm, and then said authentication device sending said new key to said AP, and sending said random number to said mobile host via said AP; (b3) said AP sending said key update message to said mobile host after receiving said new key; (C3) when receiving said random number from said authentication device and said key update message from AP, said mobile host generating a new key from said random number with the same key generation algorithm as that in step (a3); (d3) said mobile host encrypting the data packets to be sent to said AP with said new key and then sending the encrypted data packets to said AP, during the encryption process, said mobile host adding an encryption identifier to said data packets and changing the value of said encryption identifier to indicate the communication key has been changed; and (e3) when receiving the data packets from said mobile host, said AP determines whether to change the key according to value of said encryption identifier (See the rejection in claims 7 and 8 and Wang, Para 26-28.... embodiment

Art Unit: 2432

wherein AS generates the new key and sends it to the AP).

a. Referring to claim 9:

Regarding claim 9, the combination of Zhang and Wang teaches the method for distributing encryption keys in the WLAN of claim 1 wherein in order to achieve encryption communication with the new key, when receiving the data packets encrypted with the key sent from said mobile host, said AP updates the key periodically or aperiodically through the following steps of: (a4) said AP generating a new key in any way and encrypting said new key with the present key, then sending said new key to said AP, whereas sending the encrypted new key to said mobile host via said AP; (b4) after receiving said new key, said AP sending a key update message to said mobile host; (c4) when receiving the encrypted key from said authentication device and said key update message from said AP, said mobile host decrypting the encrypted key with the present key to obtain a new key; (d4) said mobile host encrypting the data packets to be sent to said AP with said new key and then sending the encrypted data packets to said AP, during the encryption process, said mobile host adding an encryption identifier to said data packets and changing the value of said encryption identifier to indicate the communication key has been changed; and (e4) when receiving the data packets from said mobile host, said AP determines whether to change the key according to value of said encryption identifier (See the rejection in claims 6,7 and 8).

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Art Unit: 2432

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to IZUNNA OKEKE whose telephone number is (571)270-3854. The examiner can normally be reached on 9:00am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/IZUNNA OKEKE/
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432